AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES LOCATED AT 600 CORAL WAY, SUITE/FLOOR 12, SEGOVIA TOWER, CORAL GABLES, FLORIDA 33134

Case No. 18-3783 JJO

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Florida
(identify the person or describe the property to be searched and give its location):

the premises located at 600 Coral Way, Suite/Floor 12, Segovia Tower, Coral Gables, Florida 33134, and any closed containers/items contained therein, as further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A.

YOU ARE COMMANDED to execute this warrant on or before 9/10/18 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/27/18 @ 2:30 pm

Judge's signature

City and state: Miami, Florida

John O'Sullivan, U.S. Magistrate Judge
Printed name and title

EXHIBIT "B"

MS_USAO_00000706

ATTACHMENT A

I. Premises to be Searched—Subject Premises

A. The premises to be searched (the "Subject Premises") are described as follows, and include all locked and closed containers found therein:

The Subject Premises is particularly described as a condominium located at 600 Coral Way, Suite/Floor 12, Segovia Tower, Coral Gables, Florida, 33134, and Any Closed Containers/Items Contained Therein. The Subject Premises occupies the entire floor.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Attachment A. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

Additionally, review of the items described in this attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. Because the owner and resident of the Subject Premises is an attorney, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privilege issues.

II. Items to Be Seized—Evidence, Fruits, and Instrumentalities of the Subject Offenses

A. Items to Be Seized

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of Title 18, United States Code, §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1344 (money laundering, conspiracy to commit money laundering, and bank fraud), related to the OneCoin business and derived funds (the "Subject Offenses"), described as follows:

a. Evidence of the Subject Offenses, including but not limited to: (i) documents and communications relating to the administration of the OneCoin business, and the transfer and/or laundering of criminal proceeds; (ii) drafts or different versions of the same; and (iii) documents and communications making reference to or containing discussion of the commission of those offenses, including those referencing the following individuals and/or entities:

- Apex Fund Services Ltd.
- B and N Consult Ltd
- Bank of Ireland
- Barclays Bank
- Barta Holdings Limited
- City National Bank
- Commerzbank
- Cryptoreal
- Deutsche Bank (Germany)
- Deutsche Bank (Cayman) Ltd.
- DBS Bank
- DMS Bank and Trust Ltd.
- DSK Bank
- Fates Group
- Fenero Equity Investments L.P.
- Fenero Equity Investments II, L.P.
- Fenero Equity Investments (Ireland), Limited
- Fenero Equity Investments (Cayman) I, L.P.
- Fenero Financial Switzerland L.P.
- Fenero Pct Holdings Limited
- Fenero Tradenext Holding Limited
- Morgan Stanley
- Mumbelli Group LLC
- Nicole Huesmann
- International Marketing Services GmBH
- International Marketing Services Pte
- MSS International Consultants (BVI), Ltd.

- MSS International Consultants LLC (together with MSS International Consultants (BVI), Ltd., "MSSI")
- OCBC Bank
- OneCoin Ltd.
- Sabadell United Bank
- Star Merchant Inc. Ltd
- United Overseas Bank

and other individuals and entities involved in the administration of OneCoin and the transfer/laundering of OneCoin fraud proceeds, covering the period of July 2015 to the present;

b. Financial agreements – including loan agreements and other documents representing purported financial contracts or obligations – memoranda and other communications, spreadsheets, ledgers, summaries, and logs relating to, or containing information regarding, transactions involving the individuals and entities described above and transactions involving any OneCoin-derived or OneCoin-related funds, covering the period of July 2015 to the present;

c. Financial records, including agreements, bank account records, corporate organization documents, ledgers, and memoranda relating to any MSSI-related and/or Fenero-related entity, covering the period of July 2015 to the present;

d. Communications constituting crimes, including emails, chats, memoranda, and/or other communications relating to the transfer and/or laundering of criminal proceeds and the transmission of funds without a license, covering the period of July 2015 to the present;

e. Communications with co-conspirators, including emails that demonstrate the relationships among co-conspirators, covering the period of July 2015 to the present;

f. Evidence concerning the identity or location of any co-conspirators;

g. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

h. Evidence sufficient to identify Mark S. Scott's use of electronic accounts, including but not limited to e-mail accounts, social media accounts, and Internet cloud storage accounts; and

i. Any items purchased by or for Mark S. Scott with funds originally sourced from OneCoin-derived or OneCoin-related proceeds, to wit:

(1) A diamond bracelet from Buchwald Jewelers;
(2) An emerald-cut engagement ring from Buchwald Jewelers;
(3) An Hermes Black Etoupe 40 bag;
(4) An Hermes Orange Poppy Birkin 35 bag;
(5) An Hermes cut clutch bag;
(6) A Big Pilot Le Petit Prince Rose Gold watch;
(7) A Panerai PAM 598 watch with blue strap;
(8) A Panerai PAM 530 watch;
(9) A Panerai PAM 421 watch;
(10) A Panerai PAM 582 barometer wall clock;
(11) A Panerai PAM 583 thermometer;
(12) A Panerai PAM 584 hygrometer watch; and
(13) A Panerai PAM 585 wall clock.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises include any computers, cellphones, electronic devices, and storage media that may contain any electronically stored information ("ESI") falling within the categories set forth above, including, but not limited to, desktop and laptop computers, cellphones (including iPhones and other smartphones), tablets (such as iPads), external hard drives, and thumb drives. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

4. Any items or records needed to access the data stored on any seized or copied computers, cellphones, electronic devices, or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

5. Any items or records that may facilitate a forensic examination of the computers, cellphones, electronic devices, or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

6. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computers, cellphones, electronic devices, or storage media.